CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

OUTILS D'ENQUÊTE SUR APPAREIL UTILISÉS PAR LA GENDARMERIE ROYALE DU CANADA ET ENJEUX LIÉS

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

John Brassard, président

NOVEMBRE 2022
44e LÉGISLATURE, 1re SESSION

OUTILS D'ENQUÊTE SUR APPAREIL UTILISÉS PAR LA GENDARMERIE ROYALE DU CANADA ET ENJEUX LIÉS

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président
John Brassard

NOVEMBRE 2022

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

John Brassard

VICE-PRÉSIDENTS

Iqra Khalid

René Villemure

MEMBRES

Parm Bains

Michael Barrett

L'hon. Greg Fergus

Jacques Gourde

Matthew Green

Lisa Hepfner

Damien C. Kurek

Ya'ara Saks

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

James Bezan

Kelly Block

Sukh Dhaliwal

Nathaniel Erkine-Smith

Ken Hardie

Arielle Kayabaga

Pat Kelly

Francis Scarpaleggia

Brenda Shanahan

Doug Shipley

Jasraj Singh Hallan

Francesco Sorbara
Rechie Valdez
Anita Vandenbeld
Ryan Williams

GREFFIÈRE DU COMITÉ

Nancy Vohl

BIBLIOTHÈQUE DU PARLEMENT

Services d'information, d'éducation et de recherche parlementaires

Sabrina Charland, Analyste
Alexandra Savoie, Analyste

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

SEPTIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)h) du Règlement, le Comité a étudié les outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada (GRC) et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE D'ACRONYMES

CPVP	Commissariat à la protection de la vie privée
CST	Centre de la sécurité des télécommunications
EASI SET	Équipe d'accès secret et d'interception des Services d'enquêtes techniques de la GRC.
ÉFVP	Évaluation des facteurs relatifs à la vie privée
GRC	Gendarmerie royale du Canada
LPRPDE	Loi sur la protection des renseignements personnels et documents électroniques
OEE	Outil d'enquête embarquée
PNIT	Programme national d'intégration de la technologie de la GRC
SCRS	Service canadien du renseignement de sécurité
SET	Services d'enquêtes techniques

SOMMAIRE

À mesure que de nouvelles technologies se développent, les défis associés à la collecte de preuves numériques par les autorités d'application de la loi, comme la Gendarmerie royale du Canada (GRC), se multiplient. Ce faisant, celles-ci doivent avoir recours à des outils d'enquête technologiques plus sophistiqués pour accéder à l'information qu'elles cherchent à obtenir dans le cadre de certaines enquêtes criminelles. Les outils d'enquête sur appareil sont un exemple d'un tel outil.

Ce rapport examine les avantages et les risques liés à l'utilisation des outils d'enquête sur appareil et l'utilisation de ce type d'outils par la GRC. Il examine aussi les mesures législatives et non législatives qui pourraient être envisagées afin de mieux encadrer l'utilisation de ce type d'outils technologiques au Canada.

À la lumière des témoignages entendus et des mémoires reçus, le Comité formule plusieurs recommandations. Ces recommandations visent à rassurer les Canadiens et Canadiennes que lorsque de nouvelles technologies sont utilisées par les autorités d'application de la loi, les lois canadiennes tiennent compte non seulement des difficultés auxquelles ces dernières font face dans l'exercice de leurs responsabilités, mais également du droit à la vie privée et de l'importance, dans une société démocratique, d'assurer le maintien de la confiance des gens envers les institutions responsables de leur protection.

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Recommandation 2

Recommandation 3

Recommandation 4

Recommandation 5

OUTILS D'ENQUÊTE SUR APPAREIL UTILISÉS PAR LA GENDARMERIE ROYALE DU CANADA ET ENJEUX LIÉS

INTRODUCTION

L'évolution des technologies utilisées par les individus qui commettent des crimes, par exemple les outils de chiffrement, fait en sorte que les forces de l'ordre, comme la Gendarmerie royale du Canada (GRC), doivent adapter leurs outils d'enquête. L'une de ces adaptations est l'utilisation d'outils d'enquête sur appareil.

Cependant, comme le présent rapport le souligne, le niveau d'intrusion que permettent ces outils et le risque qu'ils présentent en matière de protection de la vie privée soulèvent certaines inquiétudes, non seulement à l'égard de leur utilisation par les forces de l'ordre, mais aussi dans le secteur privé.

Contexte

En réponse à une question inscrite au *Feuilleton* à la Chambre des communes au sujet des programmes gouvernementaux de surveillance ou de collecte de renseignements provenant de téléphones cellulaires et d'autres appareils mobiles utilisés par les Canadiens et Canadiennes, le Leader du gouvernement à la Chambre des communes a déposé une réponse en Chambre le 22 juin 2022. La question demandait les détails de tels programmes depuis le 1 janvier 2020[1].

La réponse déposée à la Chambre des communes indique que la GRC a utilisé des outils d'enquête sur l'appareil dans le cadre d'enquêtes ciblées dans les dernières années.

1 Chambres des communes, *Ordre/Adresse de la Chambre des communes*, Q-566, 22 juin 2022, p. 3. La question écrite était la suivante : « 6 mai 2022 — M. Van Popta (Langley—Aldergrove) — En ce qui concerne les programmes gouvernementaux de surveillance ou de collecte de renseignements provenant des téléphones cellulaires et d'autres appareils mobiles utilisés par les Canadiens, y compris les programmes de données anonymisées : quels sont les détails concernant ces programmes depuis le 1er janvier 2020, y compris, pour chacun d'eux, (i) le nom du programme, (ii) la date de début du programme, si cette date est postérieure au 1er janvier 2020, (iii) une description des données recueillies, (iv) l'objectif du programme, (v) une description de la manière dont les données sont recueillies, (vi) le ministère ou l'agence responsable de surveiller le programme, (vii) le fait que le commissaire à la protection de la vie privée a été consulté ou non avant la mise en oeuvre du programme, (viii) les préoccupations soulevées par le commissaire à la protection de la vie privée, (ix) la réponse donnée à chaque préoccupation, (x) la date de fin du programme, (xi) le nombre de Canadiens dont les données ont fait l'objet d'un suivi? »

Deux programmes spécifiques de la GRC ayant mené à l'utilisation de ces outils y sont décrits : l'Équipe d'accès secret et d'interception des Services d'enquêtes techniques (EASI SET) et le Programme des Affaires spéciales « I » des Services d'enquêtes techniques[2].

En juillet 2022, à la suite du dépôt de la réponse et de la révélation des deux programmes de la GRC, le Comité a adopté une motion visant à entreprendre une étude sur l'utilisation d'outils d'enquête sur appareil par la GRC, que cette dernière appelle « outils d'enquête embarqués » (OEE).

Le Comité a tenu quatre réunions publiques et une réunion à huis clos, et il a entendu 12 témoins. Il a aussi reçu deux mémoires. Le Comité remercie tous ceux et celles qui ont participé à l'étude.

Organisation du rapport

Le rapport se divise en trois chapitres. Le chapitre 1 décrit de manière générale les logiciels espions et les différents types d'outils d'enquête sur appareil, en plus de présenter un survol des avantages et des préoccupations liées à leur utilisation. Le chapitre 2 s'intéresse plus spécifiquement à l'utilisation d'outils d'enquête sur appareil par la GRC. Le chapitre 3 discute de la modernisation du cadre législatif entourant l'utilisation de technologies de surveillance par les forces de l'ordre et d'autres. Il fait également un survol d'autres mesures qui permettraient de mieux encadrer l'utilisation de ces outils technologiques au Canada. Les recommandations du Comité se trouve à la fin du dernier chapitre.

2 Chambres des communes, *Ordre/Adresse de la Chambre des communes*, Q-566, 22 juin 2022, pp. 108-118. Selon les informations fournies dans la réponse, « les techniques et les outils de l'EASI servent principalement à recueillir des données à partir d'appareils mobiles et d'autres appareils électroniques utilisés par des suspects associés à des affaires criminelles et de sécurité nationale graves » et « les techniques du programme des Affaires spéciales "I" sont principalement utilisées pour mener des activités licites de surveillance électronique relativement à l'audio, la vidéo, la localisation et les alarmes ». La réponse indique que le programme de EASI a été créé en 2016, mais que des activités similaires ont été menées par l'équipe des opérations d'information sur le réseau de la GRC avant ce temps. Le programme spécial « I » existe depuis 1975; Gendarmerie royale du Canada, *Lettre au comité*, 16 septembre 2022. Brenda Lucki, commissaire à la GRC indique que la GRC utilise « des outils d'interception numériques de différentes sortes depuis environ deux décennies » et qu'« [e]n 2017, alors que les progrès technologiques dans la lutte contre la criminalité ne cessaient d'augmenter, la GRC a reconnu qu'il était nécessaire d'améliorer ses pratiques de gestion des dossiers centraux spécifiques et continus sur les déploiements d'[OEE] ».

CHAPITRE 1 : LES OUTILS D'ENQUÊTE SUR APPAREIL DE TYPE LOGICIELS ESPIONS

> **« [Les logiciels espions représentent] une technologie de surveillance extraordinairement puissante. N'oubliez pas que nous vivons à une époque différente de celle d'il y a 20 ans, lorsque la mise sur écoute consistait à placer un dispositif sur une ligne fixe, ou à installer un microphone ou un localisateur GPS dans la voiture d'un suspect. Ces dispositifs vous permettent de faire tout cela et plus encore, car ils sont conçus par leurs fabricants pour être aussi intrusifs que possible. »**
>
> Ronald J. Deibert,
> professeur en science politique, et directeur du Citizen Lab
> au Munk School of Global Affairs and Public Policy de la University of Toronto,
> qui a comparu devant le Comité le 9 août 2022.

Ronald J. Deibert, professeur en science politique et directeur du Citizen Lab au Munk School of Global Affairs and Public Policy de la University of Toronto, a expliqué qu'il existe de nombreux types de logiciels espions, mais que les logiciels les plus performants peuvent permettre un accès permanent, silencieux et sans limites à l'appareil d'une cible, à l'insu du propriétaire de l'appareil. Il a précisé que certaines versions plus récentes de ces logiciels espions utilisent des versions « zéro clic », c'est-à-dire qu'il n'est pas nécessaire de piéger la cible avec un lien dans un faux message. Ainsi, « un organisme gouvernemental client du logiciel espion peut simplement lancer une commande pour prendre le contrôle de n'importe quel appareil dans le monde qui est vulnérable à ce type d'exploitation ».

M. Deibert a rajouté qu'une fois dans l'appareil d'un individu, tout est possible pour l'utilisateur du logiciel. Il peut notamment intercepter et écouter des appels téléphoniques, accéder aux courriels et messages texte, qu'ils soient chiffrés ou non, activer silencieusement la caméra et le microphone de l'appareil, voir les contacts de l'individu, modifier des fichiers, accéder au nuage de données et localiser l'utilisateur de l'appareil. Selon lui, ces logiciels espions « sont conçus, ainsi que les applications qu'ils contiennent, pour espionner tous les aspects de notre vie, et constituent donc une mine d'or de renseignements à la disposition des clients des logiciels espions ». Bref, ils sont conçus par les fabricants pour être le plus intrusifs possible. Comme expliqué dans plus

de détails au chapitre 2, les outils d'enquête sur appareil utilisés par la GRC peuvent accomplir les multiples fonctions énumérées par M. Deibert lorsqu'ils sont déployés après avoir obtenu une autorisation judiciaire[3].

Avantages des outils d'enquête technologiques

Le ministère de la Sécurité publique, l'honorable Marco Mendicino, a mentionné le lien étroit entre la technologie et les services de police. Selon lui, la progression exponentielle de la technologie contraint les organismes d'application de la loi à mettre en œuvre des outils technologiques pour arriver à « poursuivre ceux qui se servent des nouvelles technologies à des fins malveillantes » de manière efficace. Il a indiqué que l'État se sert de ces outils afin de « protéger la sécurité, la paix et la santé des Canadiens ».

Sergent Dave Cobey (Serg.), du Programme de gestion des dossiers techniques et aux Services d'enquêtes techniques de la GRC, a expliqué que les outils d'enquête sur appareil peuvent aider à recueillir des preuves précieuses, puisque comme la majorité des gens, les criminels ont aussi des appareils, qu'ils utilisent d'une manière complexe. Cette nouvelle réalité n'est pas propice aux activités d'écoute électronique à l'ancienne, qui permettaient aux forces de l'ordre d'envoyer une demande à une société de télécommunications afin d'obtenir des communications. Selon Serg. Cobey, cette réalité rend essentiels les outils d'enquête sur appareil ou OEE.

Sous-commissaire Bryan Larkin (S.-comm.), des Services de police spécialisés de la GRC, a souligné que le chiffrement est essentiel dans le monde moderne, car il « protège les données financières et autres renseignements de nature délicate et permet de garantir la confidentialité des activités en ligne des Canadiens ». Cependant, il aide également les criminels à mener leurs activités illégales sans être repérés par la police. Les OEE permettent de freiner ces activités illégales en offrant aux organismes d'application de la loi, comme la GRC, la capacité de recueillir secrètement des communications privées et d'autres données qui ne peuvent plus être obtenues par des écoutes traditionnelles ou d'autres techniques d'enquête moins intrusives.

Daniel Therrien, l'ancien commissaire à la protection de la vie privée du Canada, a aussi reconnu que le chiffrement, même s'il peut avoir de nombreux avantages sociétaux et aider à la protection du droit à la vie privée des Canadiens et Canadiennes par rapport à leurs communications ou transactions commerciales, peut être un obstacle très difficile

3 Gendarmerie royale du Canada, *Outils d'enquête embarqués (OEE) Description technique Ébauche du projet*, 8 août 2022, paras 13 et 14; ETHI, *Témoignages*, Dave Cobey.

pour les organismes d'application de la loi. Selon lui « le fait de posséder une technologie adaptée aux difficultés que pose le chiffrement, moyennant une autorisation judiciaire décidée au cas par cas » est donc acceptable.

Selon Mme Polsky, présidente du Conseil du Canada de l'accès à la vie privée, la technologie elle-même est « moralement neutre ». C'est « la façon dont son utilisation est justifiée » qui détermine si elle demeure plus avantageuse que préoccupante. Elle a reconnu que les logiciels espions peuvent aider la police à effectuer son travail, mais a noté que plus souvent ils sont utilisés par d'autres acteurs à des fins malveillantes, comme le trafic humain.

Néanmoins, elle a noté que si la question est de savoir si les logiciels espions représentent des avantages sociaux, la réponse est un « oui retentissant », même si cela peut paraître contradictoire. Selon elle, ces logiciels sont

> […] la Ford Pinto de la technologie, un danger caché du public en général et de certaines personnes en particulier, avec de nombreuses retombées socialement bénéfiques sur le plan de l'emploi, du commerce et des taxes.

Mme Polsky a par exemple soulevé le fait que l'industrie mondiale de la cybercriminalité s'élève à plus de 1,5 billion de dollars américains par année et que l'industrie mondiale de la cybersécurité représente 1,7 billion de dollars américains par année, alors qu'au Canada cette industrie représente 3,5 milliards de dollars américains par année.

Préoccupations relatives à l'utilisation d'outils d'enquête technologiques

Vie privée et liberté

De nombreux témoins ont soulevé des préoccupations quant à l'utilisation d'outils d'enquête sur appareil par la GRC et d'autres entités gouvernementales, et les logiciels espions en général, surtout concernant le fait que de tels outils pourraient brimer le droit à la vie privée des Canadiens et Canadiennes et leur liberté.

Le Comité était particulièrement inquiet de l'utilisation potentielle du logiciel espion Pegasus, du Groupe NSO[4]. Dans la réponse à la question au *Feuilleton* déposée à la Chambre des Communes le 22 juin 2022, il est indiqué que la GRC utilise des outils d'enquête sur appareil dans le cadre d'enquêtes ciblées, sans toutefois mentionner le nom des logiciels utilisés.

Le ministre Mendicino a cependant rassuré le Comité que le logiciel espion Pegasus n'est pas utilisé par la GRC.

S.-comm. Larkin a lui aussi confirmé que « la GRC n'a jamais acheté ni utilisé le logiciel Pegasus ou tout autre produit de NSO ». D'autres témoins ont indiqué ne pas avoir connaissance que le logiciel Pegasus du NSO Group soit utilisé par des entités gouvernementales canadiennes ou la GRC[5].

Cependant, Michel Juneau-Katsuya, expert et chercheur sur les questions de sécurité nationale et de renseignement, a indiqué qu'il était probable que des organismes autres que la GRC, comme le Service canadien du renseignement de sécurité (SCRS) ou le Centre de la sécurité des télécommunications (CST), utilisent une technologie semblable à celle de Pegasus.

Commissaire adjoint Mark Flynn (Comm. adj.), pour la Sécurité nationale et police de protection à la GRC, a confirmé que la GRC a certains partenariats avec différents organismes de sécurité nationale, incluant le SCRS, le CST et l'Agence des services frontaliers du Canada. Toutefois, il a assuré le Comité que ces relations n'étendent pas les pouvoirs de la GRC.

Mme Polsky a souligné que plusieurs autres plateformes existent et que Pegasus n'est que le dernier logiciel espion à faire la une des journaux[6]. Mme Polsky s'est dite inquiète que ce « nouveau secteur lucratif », duquel font partie les logiciels espions, crée une incertitude pour la protection de la vie privée, la liberté et la démocratie des Canadiens et Canadiennes. Elle a rajouté que Pegasus nous rappelle que les logiciels espions sont une entreprise non partisane, et que les outils de lutte contre le terrorisme « ont fait de

4 Voir par exemple : Amnesty international, *Document de recommandations adressées à l'Union européenne en vue de mettre fin à la surveillance ciblée illégale*. Le Projet Pegasus est une collaboration de journalistes et d'organismes des droits humain, tel Amnesty international qui a été coordonnée par Forbidden Stories. Cette enquête a révélé comment les États ont ciblé des journalistes, des avocats et des personnalités politiques en ayant recours à un logiciel espion vendu par l'entreprise de cybersurveillance NSO Group : Pegasus.

5 ETHI, *Témoignages*, Philippe Dufresne; ETHI, *Témoignages*, Marco Mendicino; ETHI, *Témoignages*, Bryan Larkin; Gendarmerie royale du Canada, *Lettre au Comité* 4 août 2022.

6 ETHI, *Témoignages*, Sharon Polsky.

nous tous des proies faciles pour les attaques et l'utilisation de nos propos contre nous ».

De plus, M. Juneau-Katsuya a noté qu'en plus des logiciels espions utilisés sur des appareils mobiles, il existe d'autres formes de technologie de surveillance comme la surveillance aérienne et la surveillance par drones. Par exemple, il a indiqué que les drones sont utilisés par d'autres ministères, « particulièrement le ministère de la Défense nationale ».

D'autres témoins ont noté que même si cette étude porte sur l'utilisation de logiciel espion par la GRC, ils soupçonnent que d'autres agences gouvernementales comme le SCRS et le CST utilisent aussi des outils d'enquêtes sur appareil afin d'intercepter des communications, sans en divulguer les détails[7].

À la question de savoir si d'autres organismes ou ministères relevant de sa compétence ont utilisé des outils d'enquête sur appareil, le ministre Mendicino a affirmé que « ces techniques, si et quand elles sont utilisées, le sont toujours en conformité avec la Loi et la Charte ».

D'autres exemples des risques pour la vie privée et la liberté que peuvent présenter les outils d'enquête sur appareil et les logiciels espions ont été fournis par des témoins. Par exemple, M. Deibert a indiqué que les enquêteurs du Citizen Lab ont « documenté des préjudices et des abus importants dans presque toutes les administrations où des logiciels espions sont déployés ». Ils ont découvert que

> [l]es gouvernements utilisent de façon routinière des logiciels espions pour pirater la société civile, l'opposition politique, les journalistes, les avocats, les militants, les membres de leur famille et d'autres victimes innocentes, tant dans leur pays qu'à l'étranger, y compris des victimes qui vivent ici, au Canada.

Comme indiqué ci-dessus, l'industrie mondiale de la cybercriminalité et celle de la cybersécurité, qui peuvent impliquer l'utilisation ou la vente d'outils d'enquête sur appareil comme des logiciels espions, sont très lucratives. M. Deibert a indiqué, par exemple, que « l'industrie des logiciels espions est grandement intéressée à vendre ses produits aux forces policières locales, où les abus ont tendance à être particulièrement problématiques ».

Brenda McPhail, directrice du Programme de la vie privée, de technologie et de surveillance de l'Association canadienne des libertés civiles, a aussi soutenu que l'utilisation de ces outils encourage les forces de l'ordre à exploiter les vulnérabilités des

7 ETHI, *Témoignages*, Daniel Therrien; ETHI, *Témoignages*, Michel Juneau-Katsuya.

technologies dont nous dépendons tous, au lieu de contribuer à corriger les vulnérabilités de nos appareils et logiciels électroniques.

En fait, plusieurs témoins ont mentionné que les logiciels espions arrivent à performer en raison des déficiences de la technologie. Par exemple, Mme Polsky s'est dite préoccupée du fait que « [p]ersonne ne parle de la façon dont le logiciel espion est capable de tirer parti des lacunes et des déficiences de tant de programmes logiciels ». Elle a rappelé que nos technologies d'utilisation quotidienne sont mal équipées pour nous protéger contre les logiciels espions qui sont « tous disponibles sur le marché pour quiconque dispose d'une connexion Internet et veut les télécharger ».

M. Deibert a dit que le Citizens Lab procède régulièrement à des analyses judiciaires des victimes de logiciels espions et que dans plusieurs de ces cas, ils ont pu faire des divulgations responsables aux distributeurs de services qui ont donné lieu à des correctifs de sécurité touchant plusieurs milliards de personnes dans le monde. Il est d'avis que les organismes gouvernementaux devraient faire de même, puisque si « le gouvernement refuse de communiquer ces renseignements aux fournisseurs et met en péril notre sécurité à tous, il doit mettre une procédure adéquate en place ». Cette procédure est généralement nommée « procédure d'évaluation des vulnérabilités ».

M. Therrien était d'accord que lorsque des « représentants du gouvernement voient une vulnérabilité dans un système, ils devraient en informer le créateur ou le fournisseur du système, en tant que principe généralement applicable et mis en œuvre ».

Certains témoins ont fait remarquer qu'il y a des lacunes dans le cadre législatif applicable aux outils d'enquête sur les appareils et aux logiciels espions en ce qui concerne la protection de la vie privée, notamment le *Code criminel*, qui interdit certaines conduites et l'interception de communications sans mandat, et les lois fédérales en matière de protection des renseignements personnels. Par exemple, Mme Polsky a dit que pour autant qu'elle le sache, le *Code criminel* ne traite pas de l'installation par quelqu'un comme un conjoint, un partenaire intime ou un étranger d'un logiciel espion sur un téléphone, seulement du crime commis à l'aide du logiciel (p.ex., le partage de photos intimes). Mme McPhail et M. Therrien ont tous deux soulignés que le régime de protection des renseignements personnels du Canada a pris du retard, tant dans le secteur public que privé.

Enfin, M. Juneau-Katsuya a souligné l'importance de la protection de la vie privée telle qu'elle est définie par la *Charte canadienne des droits et libertés* et les lois canadiennes en expliquant que « cette protection est l'une des pièces centrales d'une saine démocratie et, sans elle, il n'y a pas de démocratie possible ». Il a rajouté que « la pertinence, la légalité, la légitimité et la reddition de comptes en ce qui a trait à

l'utilisation d'une ou des technologies permettant d'intercepter des conversations ou d'obtenir des informations [privées] » peuvent être protégées par la *Loi sur la protection des renseignements personnels*. Il a aussi précisé qu'en « matière d'enquête dans le domaine de la criminalité ou de la sécurité nationale, on ne peut faire valoir l'adage selon lequel « la fin justifie les moyens ». La GRC doit respecter la loi. La modernisation du cadre législatif sera discutée en plus de détails au chapitre 3.

La confiance envers les institutions et la transparence

Certains témoins ont souligné l'importance de maintenir la confiance du public dans les institutions gouvernementales et ont identifié la transparence proactive comme un moyen de favoriser cette confiance.

Philippe Dufresne, le commissaire à la protection de la vie privée du Canada, a indiqué que le Commissariat à la protection de la vie privée (CPVP) n'a pas été informé ou consulté à propos du programme de la GRC visant l'utilisation d'outils d'enquête sur appareil, avant ou depuis sa mise en œuvre. Le CPVP a pris connaissance de l'utilisation d'outils d'enquête sur appareil par la GRC dans les médias à la fin juin 2022. Il a alors communiqué avec la GRC afin d'obtenir plus de renseignements, et cette dernière a offert de faire une démonstration aux fonctionnaires du commissariat à la fin août 2022[8].

Au sujet du bénéfice de rendre publique de l'information relative à l'utilisation d'outils d'enquête sur appareil par la GRC, M. Dufresne a dit :

> [L]es répercussions de la révélation de ce type d'information par des reportages ou des questions des médias peuvent susciter des interrogations et des inquiétudes. Je pense que, du point de vue de la confiance, il serait de loin préférable que des évaluations des facteurs relatifs à la protection de la vie privée soient effectuées en amont, que mon bureau soit consulté et que cette information puisse être transmise d'une manière ou d'une autre aux Canadiens, afin qu'ils soient rassurés sur le fait qu'il existe des institutions, comme mon bureau, qui fournissent des conseils et s'assurent que la protection de la vie privée est une priorité.

Le ministre Mendicino a déclaré trouver « assez malencontreux » que le commissaire à la protection de la vie privée ait appris dans les médias que cette technique d'enquête était utilisée. M. Dufresne a dit que dans « sa réponse à la question inscrite au

8 Le Commissariat à la protection de la vie privée a, depuis 2011, une Direction de l'analyse de la technologie qui est constituée d'analystes de la recherche en technologie de l'information hautement qualifiés et qui possèdent des compétences et une expertise dans différents domaines de la technologie dont la rétro-ingénierie et l'analyse de logiciels malveillants. Commissariat à la protection de la vie privée, *Lettre au Comité*, 22 août 2022.

Feuilleton, la GRC a mentionné qu'elle avait commencé à préparer une [évaluation des facteurs relatifs à la vie privée] concernant ces outils en 2021, mais nous n'avons pas encore reçu cette évaluation ».

M. Therrien a dit ce qui suit concernant l'outil utilisé par la GRC :

> C'est l'outil lui-même qui m'a surpris, à quel point il est indiscret, et le fait qu'il était utilisé depuis si longtemps. Bien sûr, il y a eu de nombreuses discussions au fil des ans — comme la GRC l'a dit hier, cela remonte probablement au début des années 2000 — sur la question de l'accès légal. Autant pendant mon mandat comme commissaire que lorsque j'étais au ministère de la Justice, j'ai suivi ces discussions, et j'y ai aussi participé. Mais l'utilisation de cet outil en particulier pour déjouer le chiffrement, cela a effectivement été une surprise.

M. Dufresne a noté qu'assurer le respect de la protection à la vie privée est un moyen d'accentuer la confiance des Canadiens et Canadiennes envers leurs institutions. Il est d'avis que lorsque

> des organismes comme la GRC tiennent compte de l'incidence sur la vie privée dès le départ et que les Canadiens le voient, ces derniers se sentent confiants et rassurés quant à la nécessité des outils et des mesures mis en place pour atténuer l'incidence sur la vie privée et veiller à ce que les mesures et les objectifs soient proportionnels.

D'après M. Therrien, l'étude du Comité porte « sur les conditions préalables afin de donner aux Canadiens la confiance que leurs droits sont protégés lorsque des méthodes intrusives sont utilisées par les forces de l'ordre ».

Comm. adj. Flynn a dit que la GRC fourni déjà des efforts importants sur le plan de la visibilité et la transparence. Il a noté que

> des articles publics ont été publiés par des personnes comme le sergent Dave Cobey […] dans le but d'offrir une plus grande visibilité publique sur ce que nous faisons. Nous levons le voile. Nous essayons de le faire d'une manière professionnelle, qui respecte à la fois la loi sur la protection des outils et des techniques[9].

Pour sa part, le ministre Mendicino est d'avis que « des mécanismes de transparence sont en place », notamment par l'exigence de l'autorisation d'un juge de la cour supérieure, mais il a dit « rester ouverts aux suggestions visant à mettre la barre encore plus haut ». Il a ajouté qu'il faut toujours viser à faire mieux en matière de transparence. Selon lui, le rapport annuel sur la surveillance électronique représente l'un des outils

9 Gendarmerie royale du Canada, *Entrevue avec un expert en surveillance électronique sur les défis liés à la collecte de preuves*, 27 juillet 2022.

permettant de lever le voile sur la manière dont ces techniques d'enquête sont utilisées pour protéger les Canadiens et Canadiennes[10].

Comme expliqué dans le rapport annuel sur la surveillance électronique, la partie VI du *Code criminel* définit les dispositions que les services de police doivent suivre pour obtenir une autorisation judiciaire en vue d'intercepter des communications privées dans le cadre d'une enquête criminelle. L'article 195 du *Code criminel* exige que Sécurité publique Canada prépare un rapport annuel sur le recours à l'écoute électronique (en vertu de la partie VI) dans les cas de crimes pouvant faire l'objet de poursuite par le procureur général du Canada ou en son nom, et qu'il le présente au Parlement. Le rapport fournit diverses statistiques, dont le nombre de demandes d'autorisation et de renouvellement d'autorisation présentées, et la durée moyenne de validité des autorisations en nombre de jours ou d'heures[11].

Cependant, Mme McPhail était d'avis que ce rapport annuel est insuffisant puisqu'il se contente de fournir des statistiques sur toute surveillance audio ou visuelle. Elle a ajouté que sur les 331 demandes mentionnées dans le dernier rapport annuel, une seule demande de mandat a été refusée. À son avis cela laisse entendre qu'un *amicus curiae* d'intérêt public (également appelé « ami de la cour » ou « intervenant désintéressé ») devrait être présent aux audiences relatives à ces demandes d'autorisation, afin de fournir une contrepartie aux positions de la police[12].

D'autres témoins ont reconnu le besoin de plus de transparence de la GRC et du gouvernement canadien à l'égard de l'utilisation de nouvelles technologies[13].

M. Dufresne a rappelé qu'il « incombe aux organismes d'informer le commissaire à la protection de la vie privée de l'utilisation de ces outils ». Selon la directive et les politiques du Conseil du Trésor, c'est aux organismes gouvernementaux que revient l'obligation d'agir de façon proactive, par exemple en ce qui concerne la tenue d'une évaluation des facteurs relatifs à la vie privée (ÉFVP), et non au CPVP[14]. Il a indiqué que le CPVP doit être informé suffisamment à l'avance d'une ÉFVP pour qu'il puisse apporter

10 Sécurité publique Canada, *Rapport annuel sur la surveillance électronique 2020*.

11 *Ibid*. Le rapport annuel de 2020 couvre la période allant de 2016 à 2020.

12 Voir, par exemple : Ministère de la Justice, *La représentation juridique des enfants au Canada*.

13 ETHI, *Témoignages*, Ronald J. Deibert; ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Michel Juneau-Katsuya; ETHI, *Témoignages*, Daniel Therrien; ETHI, *Témoignages*, Sharon Polsky.

14 La directive du Conseil du Trésor prévoit que des ÉFVP sont faites « pour des activités ou programmes nouveaux ou ayant subi des modifications importantes nécessitant la création, la collecte ou le traitement de renseignements personnels ». Conseil du Trésor, *Directive sur l'évaluation des facteurs relatifs à la vie privée*, article 5.1.

une contribution significative. Lorsqu'une ÉFVP est effectuée après que les outils ont été en usage pour un certain temps, il est difficile de prévenir ou de résoudre les problèmes, car le CPVP est en mode réactif.

Selon M. Therrien, la GRC n'a pas été proactive dans l'amélioration de ses processus de protection de la vie privée pendant son mandat en tant que commissaire à la protection de la vie privée. Il donne l'exemple de l'utilisation de la reconnaissance faciale, qui a mené à la création du Programme national d'intégration des technologies (PNIT), non pas de manière proactive, mais à la demande du CPVP[15]. Il a rajouté que

> [s]i la Loi était plus claire quant au fait que la transparence est la règle, et qu'il est seulement acceptable de ne pas être transparent quand cela est nécessaire pour protéger les méthodes de la police, alors peut-être que les choses progresseraient.

Le ministre Mendicino a noté que le PNIT permet de rendre plus transparent en plus de centraliser et normaliser les processus qui régissent la façon dont la GRC identifie, évalue, suit et approuve l'utilisation de nouvelles technologies. Il est d'avis que ce processus centralisé permet d'assurer le respect des normes professionnelles et juridiques entourant l'utilisation de nouvelles technologies.

Selon M. Deibert, il « existe incontestablement un problème de confiance dans les institutions publiques, et nous ne sommes pas les seuls dans ce cas ». Il a entre autres réclamé des consultations publiques sur l'utilisation de logiciels espions et la divulgation de renseignement sur les logiciels utilisés, par exemple le nom du fournisseur. Il est d'avis que le processus

> [d']approvisionnement devrait être transparent et régi par des règles relatives aux fournisseurs, afin que nous ne traitions pas avec des entreprises dont les clients comprennent des gouvernements étrangers qui menacent les valeurs et la sécurité du Canada — et que nous ne contribuions pas à enrichir ces entreprises.

M. Therrien a noté que divulguer publiquement le nom des fournisseurs de services soutiendrait une meilleure transparence, dans la mesure où cette information ne rend pas les méthodes inefficaces. Assurer la transparence dans le processus d'approvisionnement est selon lui une bonne idée.

---

15 Commissariat à la protection de la vie privée du Canada, *Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée*, Rapport spécial au Parlement sur l'enquête réalisée par le Commissariat à la protection de la vie privée du Canada sur l'utilisation par la GRC de la technologie de Clearview AI et version préliminaire d'un document d'orientation conjoint à l'intention des services de police qui envisagent d'avoir recours à la technologie de reconnaissance faciale, 10 juin 2021.

M. Dufresne a de son côté reconnu qu'il « peut très bien y avoir des informations qui ne peuvent ni ne doivent être rendues publiques » en ce qui concerne les techniques d'enquête criminelle, mais selon lui, le fait de consulter le CPVP de façon confidentielle à l'égard d'une ÉFVP n'irait pas à l'encontre de ce principe.

Certains témoins se sont dit plutôt septiques à l'idée que la GRC divulgue ces informations sans en avoir l'obligation juridique. Selon Mme McPhail, la GRC semble prête à tout pour protéger le secret derrière l'utilisation de ses outils. Elle a rappelé l'affaire du projet Clemenza, qui a révélé que la GRC avait préféré abandonner un certain nombre de poursuites plutôt que d'exposer le fait qu'une clé permettant d'accéder à des informations cryptées avait été utilisée par les forces de l'ordre. M. Deibert était aussi d'avis que les autorités d'application de la loi ont tendance à être réticentes à dévoiler certaines des techniques d'enquête qu'elles utilisent.

D'ailleurs, en ce qui concerne l'utilisation d'outils d'enquête sur appareil, que décrit la réponse déposée à la Chambre des communes en juin 2022, la Commissaire de la GRC, Brenda Lucki, a refusé de partager avec le Comité les noms spécifiques des outils utilisés par la GRC, « car le fait de partager ces détails publiquement expose des informations sensibles qui pourraient avoir un impact négatif sur la capacité de la GRC et de ses partenaires à utiliser efficacement les OEE[16] ».

M. Juneau-Katsuya a appuyé l'idée que rendre publique toute l'information relative aux outils d'enquête sur appareil utilisés par la GRC pourrait être néfaste. Il a dit :

> N'oublions pas que les audiences du Comité sont publiques. Certains malfaiteurs, qu'ils soient des criminels ou des agents étrangers, écoutent ces délibérations et prennent des notes. En posant des questions dans lesquelles on insiste pour obtenir, par exemple, le pays d'origine d'une technologie qui doit rester secrète, on sert sur un plateau d'argent les moyens pour les malfaiteurs de contrer les capacités tactiques.

Bien que la GRC refuse de rendre publique la technologie qu'elle utilise par crainte de révéler des secrets sur ses outils et méthodes d'enquête au milieu criminel, M. Deibert est d'avis qu'il est important de s'assurer que « l'argent des contribuables [ne] soit [pas] versé à certaines de ces sociétés mercenaires et malhonnêtes qui contribuent à des violations des droits de la personne à l'étranger et à des problèmes de sécurité nationale ici, au Canada ». Mme McPhail s'est dite du même avis. Elle a proposé la création d'une liste d'entités de fournisseurs de logiciels espions interdits.

16 Gendarmerie royale du Canada, *Lettre au Comité*, 4 août 2022.

M. Deibert et Mme McPhail ont également soulevé le besoin de mesures de protection appropriées à la hauteur du perfectionnement et de la puissance des logiciels espions utilisés.

Enfin, S.-comm. Larkin a mentionné que la GRC reconnaît que le cadre législatif actuel comporte des lacunes et que l'organisation demeure très ouverte à travailler pour renforcir les protections, atténuer les risques, et bonifier le processus de transparence dans l'utilisation de novelle technologie.

La sécurité nationale et l'utilisation de logiciels espions par des entités étrangères

Selon M. Deibert, « l'industrie des logiciels espions mercenaires n'est pas seulement une menace pour la société civile et les droits de la personne; elle menace aussi la sécurité nationale ».

M. Deibert a rajouté que l'on en connaît très peu sur l'industrie de la technologie des armes ou du renseignement privé. Puisque ces entreprises n'aiment généralement pas divulguer publiquement ce qu'elles font ou qui sont leurs clients, M. Deibert a noté que cela rend la responsabilisation et la transparence de ces acteurs très difficiles. Dans ses recherches, le Citizen Lab a constaté

> qu'il n'existe pratiquement aucune réglementation internationale applicable à cette industrie; ces membres vendent leurs produits à n'importe quel client gouvernemental. Malheureusement, la plupart des gouvernements dans le monde sont autoritaires ou antilibéraux, et naturellement, ils n'utilisent pas cette technologie de la manière dont nous espérons qu'elle sera utilisée ici, mais pour s'en prendre à l'opposition politique, à la société civile, aux journalistes, aux militants et autres. Ils gagnent ainsi des millions de dollars et dissimulent leur infrastructure institutionnelle aux enquêteurs comme [le Citizen Lab].

Selon M. Deibert :

> Le fait est que vous possédez des appareils qui sont très invasifs et qui ont tendance à être mal sécurisés dans l'ensemble, étant donné la nature de l'écosystème numérique dans lequel nous vivons. Ces appareils coexistent avec une industrie qui, comme je l'ai décrit, dépense des millions de dollars pour trouver des failles logicielles sans les divulguer aux fournisseurs, afin de pouvoir offrir ce piratage sous forme de services. Nous avons également documenté de nombreux cas de fonctionnaires et même de chefs d'État dont les appareils ont été piratés avec les logiciels espions les plus avancés. Comme je l'ai mentionné dans ma déclaration préliminaire, nous avons observé un dispositif de piratage au 10, Downing Street, c'est-à-dire la résidence du premier ministre du Royaume-Uni, et nous l'avons signalé aux autorités britanniques.

M. Deibert a rappelé que les Canadiens et Canadiennes ne sont pas à l'abri de telle ingérence étrangère à l'aide de logiciels espions, ce qu'il qualifie de « répression numérique transnationale ». Par exemple, en 2018, le Citizen Lab a constaté que l'Arabie saoudite entreprenait des activités d'espionnage au Québec[17]. Selon M. Deibert, « les Canadiens ne sont certainement pas à l'abri de ce risque mondial qui ne cesse de croître ».

M. Deibert a noté que les recherches du Citizens Lab ont dévoilé que des gouvernements, tant autoritaires que démocratiques, avaient utilisé ce type de logiciel espion pour pirater des centaines de téléphones appartenant à des personnes à travers le monde, n'étant pas criminels ou terroristes.

M. Therrien a dit n'avoir jamais reçu de preuve d'ingérence étrangère dans la vie privée des Canadiens et Canadiennes pendant son mandat en tant que commissaire à la protection de la vie privée, mais il a indiqué avoir eu des doutes face à certaines puissances ou entreprises étrangères.

Selon Comm. adj. Flynn, le Canada est protégé de l'ingérence étrangère par des accords internationaux conclus avec certains partenaires, en particulier avec les membres du Groupe des cinq[18]. Néanmoins, il demeure préoccupant que des États étrangers qui ne sont pas des partenaires utilisent ces types d'outils et de techniques contre les Canadiens et Canadiennes.

M. Juneau-Katsuya a confirmé que, dans le passé, les autorités d'application de la loi ont eu à surveiller des membres élus à tous les échelons, municipal, provincial et fédéral, qui étaient à la solde de gouvernements étrangers. C'est ce qu'on appelle des « agents d'influence ». Ceux-ci peuvent agir consciemment ou inconsciemment, mais le résultat est le même pour la sécurité nationale et le risque auquel le Canada s'expose. Il a rajouté que depuis toujours, les agences étrangères tentent de recruter des élus et c'est relativement facile pour elles puisque les élus ne suivent malheureusement pas toujours les consignes du SCRS ou les ignorent, car ils ne servent pas leurs buts personnels et intentionnels. Il a rajouté

> [t]rès souvent, les politiciens ou les représentants élus, comme je le dis volontiers, n'étaient pas nécessairement la cible initiale, mais ont en fait attiré notre attention

17 Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak et Ron Deibert. "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil", Citizen Lab Research Report No. 115, University of Toronto, octobre 2018.

18 Le Groupe des cinq consiste en une alliance des services de renseignements et du partage de renseignement entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis. Sécurité publique Canada, *Réunion ministérielle des cinq pays*.

> lorsque nous avons constaté que des agents de renseignements étrangers ou des criminels étrangers ou canadiens étaient en contact avec eux. Le SCRS ou la GRC ont commencé à s'intéresser à ces personnes lorsqu'elles ont mené certaines activités ou accompli certains actes douteux compte tenu des responsabilités de leurs fonctions.

M. Juneau-Katsuya a aussi affirmé être inquiet du fait que certains ministres aillent travailler pour des entreprises étrangères après avoir assumé une charge publique, considérant que certaines de ces entreprises agissent directement à l'encontre des intérêts nationaux et de la sécurité nationale du Canada. Il a confirmé connaître plusieurs situations où des pays étrangers ont réussi à recruter des élus municipaux, provinciaux ou fédéraux et ont été capables d'exercer une influence de cette manière[19].

CHAPITRE 2 : LES UTILISATIONS D'OUTILS D'ENQUÊTE EMBARQUÉS PAR LA GENDARMERIE ROYALE DU CANADA

> **« Compte tenu de tous les appareils et du fait que les utilisateurs ont entièrement le choix de l'appareil qu'ils achètent, des applications qu'ils utilisent et de la façon dont ils utilisent ces applications, les OEE sont essentiels, car ils nous aident à gérer toute cette complexité. »**
>
> Dave Cobey,
> Sergent, conseiller gestion des dossiers techniques, Programme de gestion des dossiers techniques, Gendarmerie royale du Canada,
> qui a comparu devant le Comité le 8 août 2022.

Description des outils d'enquête embarqués de la Gendarmerie royale du Canada

La GRC décrit l'OEE comme étant un logiciel qui peut être déployé sur des dispositifs ou des réseaux informatiques par un accès à distance, proche ou rapproché, permettant

19 Suite à une comparution à huit-clos pour fournir au Comité plus d'information concernant l'ingérence étrangère, Mr. Juneau-Katsuya a fourni au Comité de l'information relative aux initiatives de l'Australie visant à dissuader et contrer l'ingérence étrangère: Australia Government, Department of Home Affairs, National Security, *Countering foreign interference*; Australia Government, Department of Home Affairs, National Security, Countering foreign interference, *Resources and related links* [DISPONIBLES EN ANGLAIS SEULEMENT].

ainsi la surveillance électronique [20]. Les OEE permettent d'intercepter des renseignements sur un appareil à l'insu de son propriétaire. Un OEE peut être programmé pour remplir plus d'une fonction[21].

Traditionnellement, la GRC arrivait à enquêter en interceptant des données et des communications entre deux dispositifs informatiques. Cependant, les outils de chiffrement étant devenu largement disponibles au travers d'applications répandues, tels iMessage, WhatsApp, Telegram, Signal, Kik et Skype, empêchent la GRC d'avoir recours à des techniques d'enquête traditionnelles lorsqu'elle doit obtenir accès à certaines données[22]. Les données cryptées peuvent encore être interceptées par la GRC, mais le cryptage les rend inintelligibles. « Les OEE peuvent être utilisés pour obtenir ces données dans un format lisible[23]. »

Plus spécifiquement, les OEE peuvent être déployés ou installés sur des appareils à l'insu des propriétaires des appareils et servir à :

1) recueillir/intercepter les données à l'intérieur du dispositif ciblé alors que les données ne sont pas encore cryptées;

2) collecter/intercepter les données après qu'elles ont été reçues par le dispositif et décryptées;

3) recueillir/intercepter les données avant qu'elles ne soient cryptées et envoyées;

20 Un dispositif informatique est défini par la politique de la GRC comme étant un téléphone cellulaire, un ordinateur, un serveur, une tablette ou tout autre dispositif électronique pouvant être utilisés pour envoyer ou recevoir des données sur un réseau, y compris des caméras sans fils et des serrures intelligentes. Gendarmerie royale du Canada, *Ébauche de Politique MO – Ch.*, 8 août 2022, para 1.1; La Gendarmerie Royale du Canada a fourni au Comité « Projet de politique de l'équipe d'accès secret et d'interception des Services d'enquêtes techniques (EASI) de la GRC sur la gestion des OEE et autres biens sensibles ». Gendarmerie Royale du Canada, *Lettre au Comité*, 4 août 2022.

21 Gendarmerie royale du Canada, *Ébauche de Politique MO – Ch.*, 8 août 2022, para 1.4.

22 Gendarmerie royale du Canada, *Outils d'enquête embarqués (OEE) Description technique Ébauche du projet*, 8 août 2022, para 12.

23 *Ibid.*, para 13.

4) copier secrètement des données stockées sur un dispositif ou disponibles pour cet appareil dans un stockage infonuagique[24] ou un autre périphérique de réseau;

5) capturer des données qui identifient l'utilisateur du dispositif;

6) activer les composantes périphériques du dispositif ciblé, tel que la caméra et le microphone, pour effectuer une surveillance électronique[25].

En vertu de la politique de la GRC, c'est l'EASI SET, qui est habiletés à fournir des services électroniques secrets à la GRC et à ses partenaires chargés de l'application de la loi. C'est cette équipe spécialisée qui déploie les OEE permettant l'interception de communications privées et de données de transmission, la collecte d'informations de suivi et de données au repos à partir de dispositifs informatiques. Seuls les opérateurs de l'EASI ont le droit d'utiliser les OEE au sein de la GRC[26]. Serg. Cobey a précisé que les fournisseurs de services comme Rogers, Telus ou Bell, ne sont pas impliqués dans le processus d'utilisation des OEE.

Les opérateurs de l'EASI se retrouvent dans certaines divisions ou à l'administration centrale de l'EASI, et ne peuvent utiliser d'OEE que s'ils sont certifiés pour le faire, en consultation avec le quartier général de l'EASI et avec toutes les approbations requises[27].

Seuil juridique élevé

Le ministre Mendicino et les représentants de la GRC ont indiqué que le seuil juridique pour que la GRC puisse utiliser les OEE est très élevé[28].

Le ministre Mendicino a indiqué que la GRC n'utilise que des technologies d'enquête approuvées, dans des cas d'infractions graves énumérées au Code criminel, et sur autorisation judiciaire. Le Code criminel et la loi en général comportent de nombreux mécanismes de protection qui assurent selon lui un « équilibre entre la capacité de l'État

24 Le stockage infonuagique comprend des données de transmission qui peuvent faciliter l'utilisation des OEE en dévoilant par exemple les mots de passe, les identifiants de connexion, les clés de cryptage et la configuration des systèmes et des programmes. Gendarmerie royale du Canada, *Outils d'enquête embarqués (OEE) Description technique Ébauche du projet*, 8 août 2022, para 17.

25 *Ibid.*, para 13 et 14.

26 Gendarmerie royale du Canada, *Ébauche de Politique MO – Ch.*, 8 août 2022, para 1.2.

27 *Ibid.*, paras 1.3 et 2.

28 ETHI, *témoignages*, Marco Mendicino; ETHI, *témoignages*, Dave Cobey; ETHI, *témoignages*, Bryan Larkin.

de protéger en même temps les personnes et la vie privée de l'ensemble des Canadiens ».

S.-comm. Larkin a confirmé que les « OEE sont utilisées dans des cas extrêmement rares et limités » et que « [l]eur utilisation est toujours ciblée, limitée dans le temps, et ne sert jamais à effectuer une surveillance injustifiée ou de masse ». Serg. Cobey a confirmé au Comité que depuis 2017, la GRC n'a utilisé d'OEE que dans 32 enquêtes. S.-comm. Larkin a précisé que ces 32 enquêtes n'ont ciblé que 49 appareils.

M. Juneau-Katsuya a indiqué qu'il faut faire attention face aux allégations de surveillance de masse pour deux raisons. D'abord, selon lui « rien ne prouve qu'il existe une surveillance de masse ». Ensuite, le coût élevé d'une telle opération: « Une seule opération peut facilement coûter un demi-million de dollars; je parle ici d'une opération visant à faire une interception sur une cible, peut-être à partir d'un seul appareil. » Il a rajouté que capacité opérationnelle de la GRC, du SCRS et du ministère de la Défense nationale sont très différentes de celles des capacités de l'agence de sécurité nationale américaine telles que révélées par Edward Snowden.

M. Juneau-Katsuya a également souligné que le nombre ciblé d'utilisations d'OEE au Canada, réparti sur une période de cinq ans, ne constitue pas une surveillance de masse.

M. Therrien a aussi dit ne pas croire que la GRC fait de la surveillance de masse puisqu'elle n'utilise ces outils qu'avec une autorisation judiciaire.

Serg. Cobey a rajouté que parmi les enquêtes dans lesquelles des enquêteurs ont demandé de recourir à des OEE, environ une sur dix ont donné lieu au déploiement d'OEE. Il a également spécifié les cas pour lesquels l'utilisation d'OEE a été permise dans le passé.

> La plupart des enquêtes sont liées au terrorisme ou au trafic de drogue grave. Il y a eu aussi cinq enquêtes pour meurtre et quelques enquêtes pour abus de confiance, l'une d'elles visant les activités d'un policier. Toutefois, au total, toutes catégories confondues, 32 enquêtes comportaient toutes au moins une infraction à l'article 183 […]. Ce sont toutes des infractions graves[29].

Les 32 enquêtes dans lesquelles la GRC a utilisé des OEE concernaient les infractions suivantes : importation ou trafic de stupéfiants, blanchiment d'argent, trafic de biens

29 L'article 183 du Code criminel défini le terme infraction comme « une infraction, un complot ou tentative de commettre une infraction, complicité après le fait ou le fait de conseiller à une autre personne de commettre une infraction en ce qui concerne » l'une des dispositions spécifiques du Code criminel énumérées à cet article.

criminellement obtenus, fraude, infractions liées au crime organisé, participation ou contribution à une activité terroriste, meurtre, abus de confiance par un fonctionnaire public, cybercriminalité (logiciels malveillants) et extorsion (rançongiciels), enlèvement et harcèlement criminel[30].

Autorisation judiciaire et processus interne

Plusieurs témoins ont soulevé l'importance d'exiger que la GRC obtienne une autorisation judiciaire avant d'utiliser un OEE[31].

Le ministre Mendicino a expliqué qu'il revient à un juge d'une cour supérieure de procéder « à un examen très minutieux des faits afin d'y déceler des éléments de preuve ou d'information indiquant qu'une infraction très précise a été commise ». L'autorisation d'utiliser des OEE est limitée à une liste très précise d'infractions graves figurant à la partie VI du *Code criminel*, plus spécifiquement à l'article 183. Selon le ministre,

> [l]e juge doit ensuite peser différentes considérations et établir si, entre autres choses, l'interception ou l'utilisation d'une technique quelconque est justifiée et suffisamment pressante ou urgente pour autoriser l'État à y recourir en vue d'obtenir de l'information qui sera éventuellement déposée à titre de preuve dans une procédure pénale.

Serg. Cobey a spécifié que l'utilisation d'OEE requiert l'obtention de plusieurs mandats souvent tous inclus dans une ordonnance omnibus. Par exemple, il faut un mandat d'interception des communications privées – permettant de couvrir les exigences de la Partie VI du *Code criminel*; un mandat général – requis pour le déploiement et l'utilisation de l'OEE et de la technologie en arrière-plan; un mandat d'enregistrement des données de transmission – nécessaire pour recueillir les données de transmission requises pour leur exploitation; et un mandat de localisation – seulement si l'OEE est utilisé pour recueillir des renseignements liés à l'emplacement du dispositif. Il faut également qu'une ordonnance de mise sous scellés et qu'une ordonnance d'assistance soient demandées en même temps.

Serg. Cobey a affirmé que chaque ordonnance comporte également des conditions quant à la manière de traiter les renseignements non pertinents relatifs à des tiers et à d'autres personnes, ainsi que les communications privilégiées, comme les

30 Gendarmerie royale du Canada, Réponse de la GRC, Document soumis au Comité, 15 septembre 2022. Ce document a été préparé par la GRC en réponse à une motion du Comité demandant « une liste des mandats obtenus, le cas échéant, chaque fois qu'un tel logiciel a été utilisé, précisant la portée des mandats et la raison de la surveillance effectuée ».

31 ETHI, *témoignages*, Marco Mendicino; ETHI, *témoignages*, Bryan Larkin; ETHI, *témoignages*, Mark Flynn; ETHI, *témoignages*, Dave Cobey; ETHI, *témoignages*, Michel Juneau-Katsuya.

communications liées au secret professionnel de l'avocat et autres informations de nature privée. Serg. Cobey a ajouté que dans le cas de communications entre un avocat et son client, ces conditions exigent que les renseignements soient scellés et qu'ils ne puissent être consultés sans une nouvelle autorisation du tribunal. Il a rajouté que lorsque l'autorisation judiciaire est accordée « les contrôleurs — et les analystes affectés au premier examen seraient chargés de veiller au respect des conditions [du mandat] ».

Serg. Cobey a aussi dévoilé en plus de détails le processus interne de la GRC qui mène à l'utilisation d'OEE :

> Au départ, nous organisons une consultation avec les enquêteurs qui envisagent d'utiliser ces outils. Au cours de cette consultation, nous leur expliquons — nous démystifions ces outils et expliquons — à quel point ils sont compliqués et le fait qu'ils ne vont pas forcément être en mesure de fournir les preuves qu'ils souhaitent, et nous les encourageons vraiment à envisager d'autres outils moins invasifs si possible.
>
> Tout d'abord, nous nous assurons qu'ils comprennent vraiment dans quoi ils s'engagent et qu'ils ont les ressources nécessaires pour le faire. À la suite de cette consultation, ils doivent soumettre une demande officielle de leur chaîne de commandement à nos services d'enquête[s] technique[s] afin que la direction soit informée et supervise leur demande pour s'assurer qu'elle a été correctement contrôlée.
>
> Ensuite, si cette demande est approuvée de notre côté, nous procédons à une deuxième consultation avec le procureur de la Couronne. Ou, s'ils n'ont pas de procureur de la Couronne, nous insistons pour qu'un procureur de la Couronne soit désigné afin qu'il comprenne les risques et les avantages potentiels de l'utilisation de ces outils.
>
> Nous précisons clairement au cours de cette consultation qu'il s'agit de nouvelles technologies et que nous nous attendons à ce qu'elles fassent l'objet de litiges. Nous nous assurons qu'ils comprennent le risque de litige et le genre de renseignements délicats que nous ne pouvons pas partager et que nous chercherions à protéger en vertu de l'article 37 ou de l'article 38 de la Loi sur la preuve au Canada.
>
> Tout ce processus jusqu'à présent vise vraiment à s'assurer qu'ils comprennent que s'il y a un autre outil qui fonctionne, ils devraient l'utiliser, parce que [les OEE] sont compliqués.
>
> Après toutes ces consultations, nous rédigeons une note d'engagement entre notre unité et l'unité requérante afin de consigner toutes les conversations et d'établir la nécessité de protéger les outils. Ce n'est qu'après l'accusé de réception de cette note d'engagement par l'agent responsable de l'enquête que l'assistance est fournie. Bien entendu, tout cela n'a aucune importance à moins qu'une autorisation judiciaire n'ait été accordée par le biais du processus que nous avons décrit précédemment en ce qui concerne un représentant de la Couronne, une autorisation en bonne et due forme avec toutes les conditions que nous avons précisées.

Comm. adj. Flynn a rajouté qu'il existe des mesures de protection supplémentaires dans les politiques et procédures d'utilisation d'OEE pour certains secteurs. Il a notamment nommé les parlementaires, les journalistes, les institutions religieuses et les établissements d'enseignement. Ainsi, un niveau d'autorisation beaucoup plus élevé est requis lorsqu'une demande de surveillance électronique est soumise à l'égard d'une personne œuvrant dans ces secteurs.

Selon l'expérience de M. Juneau-Katsuya, ce n'est pas toujours le même juge qui procède à l'évaluation, mais certains sont spécifiquement sélectionnés en raison du degré de confidentialité et du niveau de sécurité nationale de l'information qu'ils devront consulter. Néanmoins, M. Deibert a indiqué se demander, avec tout le respect qu'il doit aux juges envers desquels il a confiance, s'ils comprennent vraiment la portée, l'échelle, le degré de sophistication et la puissance du type de technologie intrusive faisant l'objet de l'étude du Comité.

M. Therrien a dit croire que les juges qui évaluent les demandes d'autorisation judiciaire ont l'expertise technique et juridique pour prendre la meilleure décision. Il a souligné que les juges sont « liées par les dispositions de la partie VI du *Code criminel* » lorsqu'ils évaluent une demande de mandat, mais que

> [l]e Commissariat à la protection de la vie privée examine de façon plus générale la protection de la vie privée en vertu de sa loi; il peut donc fournir une assurance supplémentaire au public que la vie privée, au-delà de ce qui est prévu dans le Code criminel, sera respectée quand ces outils seront utilisés.

M. Therrien « ne croi[t] pas que la GRC est une organisation rebelle ». Il reconnaît que la GRC n'utilise les OEE que sur autorisation judiciaire, mais est d'avis qu'il serait une bonne idée d'avoir un processus d'audit pour s'assurer que l'agent de police qui effectue la tâche en question le fasse en respectant les exigences de la Cour. Comme indiqué ci-dessus, la GRC dispose d'un processus interne pour s'assurer que les demandes d'OEE sont surveillées et que les conditions du mandat obtenu sont respectées.

Pour sa part, Comm. adj. Flynn est d'avis que les évaluations des juges « tiennent absolument compte du facteur protection de la vie privée ». S.-comm. Larkin a rajouté que les « juges reçoivent des documents d'accompagnement expliquant ce qu'est l'OEE et ses capacités ».

Évaluation des facteurs relatifs à la vie privée

S.-comm. Larkin a confirmé qu'aucune ÉFVP n'avait été complétée par la GRC à l'égard de son utilisation d'OEE au moment où les représentants de la GRC ont comparu devant le Comité.

Selon M. Therrien, le caractère extrêmement intrusif de l'utilisation d'OEE aurait dû donner lieu à une ÉFVP. Plusieurs témoins étaient du même avis[32].

En ce qui concerne le besoin de faire une ÉFVP, Comm. adj. Flynn a souligné que la vie privée se trouve surtout dans le contenu de l'information et non dans la méthode d'obtention de cette information, peu importe qu'il s'agisse de l'interception d'une communication analogue ou d'une communication cryptée. Ainsi, le seuil de déclenchement pour procéder à un PIA n'est pas toujours évident. Avec le temps la GRC change parfois sa position sur ces questions.

Comm. adj. Flynn a expliqué que la GRC considère que l'atteinte réelle à la vie privée consiste en l'action d'écouter une conversation ou d'observer physiquement une personne. Comme ce type d'intrusion se produit depuis des années (à l'aide de différentes méthodes), il ne s'agit donc pas d'un nouveau type d'intrusion à la vie privée. L'OEE n'est qu'une nouvelle méthode utilisée, mais pas une nouvelle atteinte à la vie privée.

Comm. adj. Flynn a réitéré que l'atteinte à la vie privée ne provient pas de l'outil utilisé pour intercepter des communications, mais de la « capture de l'audio ou du message texte ou de la communication entre deux personnes » et que « [la GRC a] évolué dans l'utilisation des outils à mesure que les individus ont évolué dans leur façon de communiquer ».

Serg. Cobey a aussi noté que la protection de la vie privée des tiers innocents et des communications non pertinentes est un problème qui n'est pas unique à l'OEE, mais qui existe depuis l'arrivée des premières technologies d'écoute électronique.

Mme McPhail a critiqué le fait que la GRC n'envisage pas d'effectuer une ÉFVP simplement parce qu'elle utilise une nouvelle technologie, mais seulement si la technologie permet un nouveau type d'intrusion. Elle a souligné que cette approche ne tient pas compte de la réalité d'un OEE, « qui permet toutes les intrusions en même temps sur un appareil », comme enregistrer les sons en direct, surveiller les

32 ETHI, *Témoignages*, Philippe Dufresne; ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Ronald J. Deibert; ETHI, *Témoignages*, Sharon Polsky; et ETHI, *Témoignages*, Michel Juneau-Katsuya.

emplacements, recueillir les identifiants des appareils, enregistrer les recherches Internet, et suivre l'utilisation des applications. Elle a expliqué :

> Pratiquaient-ils des écoutes auparavant? Bien sûr. Ces écoutes permettaient-elles d'accéder au contenu de toute forme de communication écrite et orale, professionnelle et privée, rétrospectivement et prospectivement, y compris les données qui ne se trouvent pas sur l'appareil même, mais dans le nuage? Bien sûr que non. S'agit-il du même niveau d'intrusion? Non. La police a-t-elle installé des caméras cachées dans des maisons et des lieux d'affaires après avoir obtenu un mandat par le passé? Bien sûr. Une seule caméra avait-elle la capacité de se déplacer avec un sujet d'enquête du travail à la maison, de la chambre à la salle de bain, 24 heures sur 24? Bien sûr que non. S'agit-il du même niveau d'intrusion? Non.

Cependant, les fonctions des OEE utilisées par la GRC peuvent varier. Certains OEE permettent un contrôle à distance interactif complet du dispositif ciblé. D'autres types d'OEE font appel à un serveur de l'EASI et attendent les commandes pour être exécutées. Par exemple, un OEE peut être configuré pour contacter le serveur de l'EASI à toutes les cinq heures. S'il y a des commandes en attente, il les exécute. Sinon, il ne fait rien. En ce qui concerne la possibilité d'activer le microphone d'un dispositif ciblé, le contrôle du collecteur du microphone activité diffère selon l'OEE, le système d'exploitation de l'appareil et le service de télécommunications[33].

M. Therrien a lui aussi souligné le fait « que cet outil en particulier est extrêmement indiscret, bien plus que les outils d'écoute électronique habituels ». Il a noté que lorsqu'un tel outil est installé l'appareil numérique d'une personne, « l'État — la police — a accès à tout ce qui se trouve sur le téléphone. C'est extrêmement indiscret. »

D'autres témoins ont partagé l'avis que cette technologie de surveillance est beaucoup plus intrusive que l'écoute électronique et d'autres technologies précédemment utilisées. Compte tenu de la nature de ces outils, Mme McPhail a affirmé que « même une EFVP ne suffit pas face à l'énormité de cette intrusion ».

33 Gendarmerie royale du Canada, *Outils d'enquête embarqués (OEE) Description technique Ébauche du projet*, 8 août 2022, paras. 18(e) et 25.

CHAPITRE 3 : LA MODERNISATION DU CADRE LÉGISLATIF ET AUTRES MESURES

> **« La protection de la vie privée et l'intérêt public vont de pair. Ils tirent parti l'un de l'autre, se renforcent mutuellement, et les Canadiens et leurs institutions ne devraient pas avoir à choisir entre l'un ou l'autre. »**
>
> Philippe Dufresne,
> Commissaire à la protection de la vie privée,
> qui a comparu devant le Comité le 8 août 2022.

Plusieurs témoins ont souligné l'importance d'apporter différentes modifications au cadre législatif qui s'applique à l'utilisation de logiciels espions et d'outils d'enquête sur appareil.

Par exemple, le ministre Mendicino s'est dit ouvert aux suggestions pour renforcer les mécanismes de transparence pour raffermir la confiance des Canadiens et Canadiennes. M. Therrien a affirmé que « les conditions préalables à la confiance sont des règles juridiques claires, des normes juridiques élevées et une surveillance indépendante ».

Modernisation et bonification de la Partie VI du *Code criminel*

M. Dufresne a indiqué que la Partie VI du *Code criminel* comprend certaines conditions qui visent à protéger la vie privée tout en permettant la tenue d'enquêtes criminelles. Notamment, il a mentionné que cette partie du *Code criminel* prévoit les circonstances dans lesquelles l'outil pourra être utilisé par les forces policières, l'obligation d'obtenir l'autorisation d'un juge, l'obligation de donner des notifications, ainsi que plusieurs autres critères.

M. Dufresne a toutefois noté que bien que la Partie VI du *Code criminel* contienne un certain nombre de garanties, cela « n'enlève pas la nécessité, pour les forces policières, lorsqu'elle prévoit utiliser de nouveaux outils, de faire une vérification des répercussions qu'ils pourraient avoir en matière de vie privée ». Selon lui, il est donc possible que le régime applicable doive être bonifié afin d'y ajouter d'autres critères ou mécanismes.

M. Dufresne a expliqué la différence entre l'autorisation judiciaire et l'ÉFVP :

> Le mandat approuvé par le juge permettra d'examiner la demande particulière selon les critères du Code criminel et de suivre ce processus. L'EFVP permettra d'examiner la

> situation du point de vue du programme. Dans le cadre de l'évaluation, on examinera de façon générale les types d'outils disponibles qui sont utilisés, les mécanismes qui permettent d'autoriser l'utilisation de ces outils et la question de savoir si ces mécanismes sont suffisants. Par exemple, devrait-il y avoir des exigences différentes ou supplémentaires avant que leur utilisation judiciaire puisse être autorisée, ou devrait-il y avoir, en plus de l'autorisation judiciaire, des mécanismes pour protéger l'information? Cela n'est peut-être pas nécessaire, mais l'EFVP sert à cela, c'est-à-dire à examiner la situation, non pas par rapport à un cas particulier, mais par rapport à l'ensemble du programme.

M. Therrien a aussi noté que la partie VI du *Code criminel* offre un cadre juridique qui comprend des normes exigeantes et une surveillance indépendante par des tribunaux. Toutefois, il est selon lui possible de bonifier ce cadre juridique de manière proactive, par exemple en ce qui a trait aux ÉFVP[34]. Il a expliqué que la Partie VI du *Code criminel* énonce les normes relatives à la vie privée que le tribunal doit appliquer lorsqu'il octroie un mandat. Cependant, cette définition de la vie privée est beaucoup moins large que celle retrouvée dans la *Loi sur la protection des renseignements personnels*. Par conséquent, bien que les cours jouent leur rôle adéquatement en vertu du *Code criminel*, cela ne veut pas dire qu'une ÉFVP n'a pas aussi un rôle à jouer pour assurer une meilleure protection de la vie privée des Canadiens et Canadiennes.

Mme McPhail, M. Deibert et M. Juneau-Katsuya ont tous indiqué que la Partie VI du *Code criminel* n'a pas suivi le rythme du développement de la technologie du monde criminel et aurait besoin d'être mise à jour par le gouvernement.

Par exemple, Mme McPhail a soulevé l'importance « d'examiner la Partie VI du *Code criminel* qui […] n'a pas subi de modifications significatives depuis un peu plus de 20 ans ». Elle a noté qu'il serait utile pour des experts de l'utilisation de cette partie du *Code criminel* d'être invité à signaler les améliorations qui devraient y être apportée afin de tenir compte des changements fondamentaux que connaît la technologie.

Modernisation de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et documents électroniques*

Plusieurs témoins ont souligné que les lois fédérales en matière de protection des renseignements personnels devraient être améliorées. Par exemple, Mme McPhail a

34 ETHI, *Témoignages*, Daniel Therrien.

affirmé qu'il existe des lacunes dans les lois protégeant la vie privée tant dans le secteur privé que public.

M. Therrien a expliqué qu'en 2022 l'information circule largement entre le secteur privé et public, c'est pourquoi il est important que les lois du secteur public et du secteur privé soient compatibles et complémentaires. Selon lui, « [i]déalement, elles devraient être réunies en une seule loi, car les données ne connaissent pas de frontières entre le secteur public et le secteur privé ». M. Therrien a reconnu que « le contexte est un peu différent parfois », mais il a soutenu que « les lois devraient avoir des principes semblables, sinon identiques » entre le secteur public et privé.

Cependant, M. Therrien a indiqué ne pas croire qu'une telle réforme soit réalisable dans un délai raisonnable, considérant qu'il a fallu attendre 40 ans avant pour avoir des modifications à la *Loi sur la protection des renseignements personnels* et 20 ans pour des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[35]. Il a donc dit que le « risque de tout mettre dans une loi au Canada aujourd'hui serait de retarder l'adoption de la loi relative au secteur privé [projet de loi C-27], qui est présentement devant le Parlement[36] ».

M. Therrien a rajouté que

> [n]ous devrions nous assurer que le Commissariat à la protection de la vie privée du Canada, tant pour le secteur public que pour le secteur privé, a le pouvoir de non seulement faire des recommandations, mais de rendre des ordonnances pour le secteur privé et le secteur public lorsqu'il constate des violations de la Loi. Il devrait aussi y avoir des sanctions financières, certainement dans le secteur privé, pour que l'on s'assure que ces lois sont respectées.

M. Dufresne, M. Therrien et Mme McPhail ont recommandé que les lois fédérales en matière de protection des renseignements personnels reconnaissent que la protection de la vie privée est un droit fondamental.

M. Therrien a indiqué qu'incorporer des normes juridiques claires, tel un droit fondamental à la vie privée, dans le préambule de la *Loi sur la protection des renseignements personnels* permettrait de mieux définir l'approche canadienne en matière de protection à la vie privée. Il a ajouté que même si le préambule d'une loi n'a

35 ETHI, *Témoignages*, Daniel Therrien.

36 Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, 44e Parlement, 1e session. Le projet de loi a été déposé à la Chambre des communes le 16 juin 2022.

pas de force exécutoire en soi, il est un outil précieux dans l'exercice d'interprétation. Il a expliqué, par exemple, en ce qui concerne la *Loi sur la protection des renseignements personnels*, que

> [s]i le préambule énonce que la protection de la vie privée est un droit fondamental essentiel pour protéger la dignité des personnes, alors quand la GRC, le ministère de la Santé ou n'importe quelle autre organisation va effectuer une EFVP, les gens vont garder ce message important en tête.

M. Dufresne s'est aussi dit en faveur d'insérer un préambule dans la *Loi sur la protection des renseignements personnels* qui soulignerait l'importance fondamentale de la protection de la vie privée pour la dignité et les droits des Canadiens et Canadiennes. Selon lui, nous devrions avoir au sein des institutions fédérales, une culture de protection de la vie privée.

M. Therrien a suggéré que la protection de la vie privée dès la conception devrait être une norme de pratique dans l'adoption de toutes nouvelles technologies par les autorités d'application de la loi. M. Therrien a décrit la protection de la vie privée dès la conception comme un processus qui intègre des considérations à la protection de la vie privée avant l'utilisation d'une technologie particulièrement indiscrète. Les avantages de tenir compte de la protection de la vie privée dès la conception sont d'assurer la population que les violations ne seront pas seulement découvertes après coup et de grandement réduire le nombre de violations grâce au processus mis en place.

M. Dufresne a lui aussi mentionné que « la protection de la vie privée devrait être prise en compte dès la conception ». Cela ferait en sorte que lorsque de nouveaux outils sont envisagés, la priorité soit donnée à l'examen des répercussions qu'ils pourraient avoir sur la vie privée.

M. Dufresne a précisé qu'à l'heure actuelle, même si la directive du Conseil du Trésor[37] exige des ÉFVP dans le cadre de ses politiques, « la Loi sur la protection des renseignements personnels ne prévoit pas que la GRC ou toute autre institution gouvernementale doive réaliser des évaluations des facteurs relatifs à la vie privée ». Il a indiqué qu'il espère que cette exigence sera incluse comme une obligation juridique dans une version modernisée de la *Loi sur la protection des renseignements personnels*.

M. Dufresne a noté que tenir compte de l'incidence sur le respect de la vie privée dès le début, par exemple en consultant le CPVP, permettrait de prévenir les atteintes à la vie privée et améliorer les outils servant à promouvoir l'intérêt public, qu'il s'agisse de la

37 Conseil du Trésor, *Directive sur l'évaluation des facteurs relatifs à la vie privée*.

prévention du crime, de la protection de la sécurité nationale ou du renforcement de la compétitivité du Canada.

Par exemple, dans le cas de l'utilisation d'outils d'enquête sur appareil par la GRC, M. Dufresne a expliqué :

> Lorsque nous recevrons l'EFVP, nous l'examinerons pour nous assurer qu'elle comprend une évaluation significative de la conformité du programme en matière de protection des renseignements personnels ainsi que des mesures pour atténuer les risques d'atteinte à la vie privée. Nous examinerons également l'EFVP pour nous assurer que tout programme ou activité portant atteinte à la vie privée est légalement autorisé, qu'il est nécessaire pour répondre à un besoin précis et que l'atteinte à la vie privée causée par le programme ou l'activité est proportionnelle aux intérêts publics en jeu. La GRC devrait donc déterminer s'il existe un moyen moins intrusif d'atteindre le même objectif. Si nous constatons des lacunes en matière de protection de la vie privée, nous communiquerons nos recommandations à la GRC et nous nous attendrons à ce qu'elle apporte les changements nécessaires.

Selon M. Dufresne, les ÉFVP sont un outil important pour une culture de protection de la vie privée, car elles permettent de prendre l'habitude de se poser des questions, par exemple à savoir si l'utilisation d'un certain outil est nécessaire ou si autant de renseignements sont nécessaires pour atteindre un objectif.

D'autres témoins étaient aussi d'avis qu'il est important d'intégrer l'obligation d'effectuer une ÉFVP dans la loi[38].

Selon M. Therrien, il ne faudrait pas seulement instaurer une obligation juridique de consulter le CPVP, mais aussi préciser dans la loi les circonstances dans lesquelles une ÉFVP doit avoir lieu. Il a rappelé, par exemple, qu'en ce qui concerne l'utilisation d'outils d'enquête sur appareil, la GRC ne semble rien voir de nouveau quant au fait qu'elle utilise cette technologie. Il faudrait donc préciser, en termes généraux,

> le moment où ces évaluations doivent être faites et dans quel but elles doivent l'être. Ainsi, on pourrait s'assurer, de façon proactive, que la loi est respectée. Il n'y aurait pas seulement un examen ex post facto, mais aussi un examen préalable pour s'assurer que la loi est respectée.

M. Juneau-Katsuya et M. Deibert ont aussi reconnu que le CPVP devrait être impliqué dans le processus menant à l'utilisation, par les forces de l'ordre, de nouveaux outils technologiques. Par exemple, M. Deibert s'est dit « très déçu d'entendre que le [CPVP] n'était pas informé de l'utilisation de ces techniques d'enquête avant les récentes

38 ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Ronald J. Deibert; ETHI, *Témoignages*, Sharon Polsky.

révélations ». Il a recommandé de fournir aux commissaires à la protection de la vie privée plus de capacités et de ressources afin qu'ils puissent assurer une meilleure surveillance des organismes responsables de la sécurité[39].

M. Dufresne a aussi noté l'importance de bien évaluer les risques et la nécessité d'avoir recours à l'utilisation d'un certain outil, et recommandé l'adoption des critères de nécessité et proportionnalité pour justifier une telle utilisation.

Enfin, certains témoins ont aussi soulevé l'importance d'incorporer une obligation de transparence dans la loi. M. Deibert est d'avis que les forces de l'ordre devraient divulguer l'information sur la technologie qu'elles se procurent. M. Therrien a suggéré l'adoption de la norme suivante en matière de transparence : « [L]e gouvernement et la police [ont] l'obligation d'être transparents, excluant seulement ce qui est nécessaire pour protéger les méthodes de la police et l'intégrité des enquêtes. »

Moratoire ou interdiction générale

Certains témoins se sont prononcés sur la possibilité d'imposer un moratoire sur l'utilisation de logiciels espions au Canada.

Mme McPhail a affirmé qu'un moratoire est nécessaire. Mme Polsky n'était pas opposée à l'idée d'un moratoire, mais a noté qu'il ne s'agit d'une mesure temporaire. Elle a indiqué « que le risque est plus grand que la récompense » avec les logiciels espions. Selon elle, l'utilisation des logiciels espions devrait tout simplement être illégale, à la seule exception de situations particulières et bien définies par la loi. Elle a affirmé qu'il ne faut pas seulement en interdire l'utilisation par la police.

Mme McPhail a souligné qu'une brève interruption d'utilisation d'un outil soi-disant « de dernier recours » ne devrait pas constituer un grand risque pour la sécurité publique comparativement aux risques que son utilisation impose aux droits à la vie privée, à l'application de la loi, ainsi qu'aux répercussions sociales et diplomatiques. Elle a rajouté que si un moratoire n'est pas imposé, de sérieuses modifications législatives doivent être apportées. Elle est aussi d'avis que le Canada devrait suivre l'exemple des États-Unis et de l'Europe en bannissant l'achat de logiciels espions par l'État.

Mme McPhail a aussi indiqué que le Canada devrait envisager de créer une liste d'entités de fournisseurs de logiciels espions interdits similaire à celle des États-Unis. Une telle liste offrirait au public une certaine assurance que l'argent de leurs impôts ne

39 Comme indiqué ci-dessus, le Commissariat à la protection de la vie privée a une Direction de l'analyse de la technologie depuis 2011.

va pas soutenir ces entreprises dangereuses et mercenaires. Sur ce point, le ministre Mendicino s'est dit prêt à interdire le logiciel Pegasus au Canada.

D'autres témoins n'étaient pas en faveur d'une interdiction complète des logiciels espions. Par exemple, M. Therrien a dit qu'il faudrait réguler la vente, l'importation et l'exportation de ces technologies sans nécessairement en interdire complètement l'utilisation.

Toutefois, M. Therrien a dit que « même si le gouvernement, l'État et la police ont des motifs légitimes d'utiliser exceptionnellement ce type de technologie avec une autorisation judiciaire », il « ne trouve vraiment aucune raison valable pour laquelle une personne du secteur privé devrait pouvoir utiliser cette technologie ». Mme Polsky et M. Juneau-Katsuya ont abondé dans le même sens.

Mme Polsky a indiqué qu'il ne s'agit pas simplement de bannir l'utilisation des outils technologiques par les forces de l'ordre, qui peut être légitime. Le problème réside dans le fait que ces outils sont disponibles sur le marché. M. Juneau-Katsuya a dit :

> J'aimerais simplement ajouter que nous passons beaucoup de temps à parler des forces de l'ordre, qui est le leitmotiv de cette discussion, mais que nous avons omis de parler du monde privé. Les entreprises privées utilisent beaucoup plus ce type de technologie que les forces de l'ordre, qui sont beaucoup plus surveillées.

M. Dufresne a préféré ne pas se prononcer sur l'imposition d'un moratoire pour le moment vu le manque d'information sur les logiciels utilisés par la GRC. Il a plutôt rappelé au Comité l'importance pour le CPVP « de déterminer quelles sont les répercussions de l'utilisation de tels outils et ses implications, puis de faire des recommandations en fonction des renseignements fournis par la GRC ». La GRC devait tenir une réunion avec le CPVP à la fin août 2022 pour leur offrir une démonstration de l'utilisation d'OEE. Aucun renseignement supplémentaire à l'égard de cette démonstration n'a été fourni au Comité à la suite de la comparution de M. Dufresne.

Enfin, selon Comm. adj. Flynn, les lois du Canada ont protégé le droit à la vie privée, sans égard au degré de sophistication requis par la GRC pour remplir leur devoir. Il est d'avis que ces protections sont valables aujourd'hui, comme elles l'étaient dans les années 1960. Il est donc contre l'imposition d'un moratoire sur l'utilisation de logiciels espions.

Autres mesures

Certains témoins ont recommandé des mesures non législatives pour mieux encadrer la vente et l'utilisation de logiciels espions, de même qu'augmenter la sensibilisation à la protection de la vie privée.

Par exemple, Mme Polsky a proposé qu'une stratégie d'éducation pancanadienne soit élaborée afin d'apprendre aux étudiants, jeunes et universitaires, à mieux comprendre les principes de base de la vie privée en ligne, comment elle peut être compromise et comment se protéger.

M. Deibert a insisté sur le besoin d'informer les Canadiens et Canadiennes et tenir des audiences publiques sur les dangers liés à l'industrie des logiciels espions mercenaires.

M. Deibert a aussi suggéré que le Canada mette en place de solides mesures de contrôle des exportations pour l'industrie de la surveillance canadienne, puisqu'à l'heure actuelle, il n'y en a aucune. Il est d'avis que le Canada devrait également pénaliser les fournisseurs de logiciels espions qui sont connus pour faciliter les violations des droits de la personne à l'étranger de sorte que ces pénalités suivent le modèle américain. Selon lui, le Canada devrait aussi élaborer des lignes directrices d'approvisionnement pour les organismes canadiens afin qu'ils ne passent jamais de contrats avec des entreprises liées à des violations des droits de la personne à l'étranger.

M. Juneau-Katsuya a reconnu que la Chambre des communes a créé un comité permanent sur la sécurité et le renseignement, qui est capable d'aller dans tous les ministères pour remonter la piste de certaines affaires. Il a noté que la difficulté avec un tel comité est que ses membres sont élus, et peuvent changer à chaque élection. Il a cependant critiqué le Comité de surveillance des activités de renseignement de sécurité « qui était un chien de garde et qui, au fil du temps, a fini par devenir un chien de poche » puisqu'il ne peut faire tout le travail nécessaire pour observer et critiquer les problèmes dans le domaine de la sécurité, et y apporter des solutions.

Dans le même sens, Mme McPhail a soulevé que pour contrer la tendance persistante de la police à acquérir et à utiliser des technologies de surveillance sophistiquées et potentiellement controversées sans en informer le public, le gouvernement canadien pourrait suivre l'exemple de l'État de New York et de la Nouvelle-Zélande en mettant sur pied un comité consultatif indépendant composé d'intervenants pertinents de la communauté juridique, du gouvernement, de la police, de la sécurité nationale, de la société civile et, bien entendu, des organismes de réglementation pertinents, comme le CPVP.

Selon Mme McPhail, ce comité consultatif

> pourrait servir d'organisme national d'établissement de normes, d'organisme consultatif, et examinerait de manière proactive les types de technologies que nos forces de police souhaitent utiliser pour moderniser leurs techniques d'enquête et les étudier en tenant compte de toute une série de considérations, y compris des considérations éthiques et juridiques, et des considérations liées aux normes et valeurs canadiennes. Il pourra ensuite recommander des normes, des normes d'excellence, aux organismes policiers, non seulement à l'échelle nationale, mais aussi à l'échelle provinciale et territoriale — car, bien entendu, le maintien de l'ordre est aussi une question provinciale et territoriale — afin d'assurer une certaine uniformité et de garantir au public que les droits sont respectés et que les policiers disposent des outils dont ils ont besoin pour accomplir leur travail difficile.

Mme McPhail a affirmé que comme le maintien de l'ordre relève des provinces et des territoires, un ensemble hétéroclite de lois pertinentes existent. Il peut donc être plus difficile de s'assurer que tous les services de police du pays se conforment à des normes optimales en matière d'utilisation des technologies de surveillance. Le comité consultatif fédéral qu'elle a proposé pourrait remédier à ce problème en établissant des pratiques exemplaires.

D'après M. Deibert, certains membres des plus hauts échelons du gouvernement canadien, tels les hauts fonctionnaires, le premier ministre, le ministre de la Sécurité publique et la ministre des Affaires étrangères, devraient aussi déclarer clairement et avec force que l'industrie de technologie de surveillance est une menace pour les droits de la personne, la démocratie et la sécurité nationale. Cette déclaration devrait affirmer que le Canada prévoit prendre des mesures, en collaboration avec ses alliés aux États-Unis, en Europe et dans le monde, pour demander des comptes aux pires acteurs de l'industrie, et qu'il entend être plus transparent et rendre davantage des comptes au public si cette technologie doit être utilisée au niveau national.

Enfin, M. Deibert a recommandé que le Canada impose aux personnes ayant travaillé dans les organismes de sécurité nationale canadiens une interdiction à vie de travailler avec des sociétés de logiciels espions mercenaires.

OBSERVATIONS ET RECOMMANDATIONS DU COMITÉ

La plupart des membres du Comité tiennent d'abord à soulever le manque de coopération dont a fait preuve la GRC dans le cadre de cette étude. Le Comité n'est pas satisfait des réponses qu'elle a fournies à ses questions.

Le Comité reconnaît qu'il existe un vide juridique entourant l'utilisation de nouveaux outils d'enquête technologiques. Il est donc d'avis qu'un meilleur cadre juridique entourant l'utilisation d'outils d'enquête sur appareil par la GRC est nécessaire pour assurer une utilisation appropriée de ce type d'outils et le maintien du droit à la vie privée des Canadiens et Canadiennes.

À la lumière de ce qui précède, le Comité recommande :

Recommandation 1

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure une obligation explicite pour les institutions fédérales de faire des évaluations des facteurs relatifs à la vie privée avant d'adopter des outils technologiques à haut risque qui font la collecte de renseignements personnels et de les soumettre au Commissariat à la protection de la vie privée du Canada pour évaluation.

Recommandation 2

Que le gouvernement du Canada crée une liste de fournisseurs de logiciels espions interdits et qu'il établisse des règles claires en matière de contrôle des exportations de technologies de surveillance.

Recommandation 3

Que le gouvernement du Canada révise la Partie VI du *Code criminel* afin de s'assurer qu'elle est adaptée à l'ère numérique.

Recommandation 4

Que le gouvernement du Canada modifie le préambule de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et documents électroniques* afin d'indiquer que le droit à la vie privée est un droit fondamental.

Recommandation 5

Que le gouvernement du Canada rappelle régulièrement aux anciens membres élus ou nommés ou à toute personne ayant déjà travaillé pour une agence de sécurité nationale leurs obligations à vie en vertu de la *Loi sur la protection de l'information* et obtienne de leur part une reconnaissance de leur compréhension de ces obligations.

Recommandation 6

Que le gouvernement du Canada accorde au Commissariat à la protection de la vie privée du Canada le pouvoir de faire des recommandations et de rendre des ordonnances, tant dans le secteur public que le secteur privé, lorsqu'il constate des violations des lois dont il est responsable.

Recommandation 7

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'inclure le concept de protection de la vie privée dès la conception et une obligation pour les institutions fédérales qui y sont assujetties de respecter cette norme lorsqu'elles développent et utilisent de nouvelles technologies.

Recommandation 8

Que le gouvernement du Canada mette sur pied un comité consultatif indépendant composé d'intervenants pertinents de la communauté juridique, du gouvernement, de la police et de la sécurité nationale, de la société civile et des organismes de réglementation pertinents, comme le Commissariat à la protection de la vie privée du Canada, afin d'examiner les nouvelles technologies utilisées par les forces de l'ordre et d'établir des normes nationales concernant leur utilisation.

Recommandation 9

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure des exigences explicites en matière de transparence pour les institutions fédérales, sauf lorsque la confidentialité est nécessaire pour protéger les méthodes utilisées par les autorités d'application de la loi et assurer l'intégrité de leurs enquêtes.

CONCLUSION

Toute technologie intrusive comme les outils d'enquête sur appareil méritent d'être bien encadrés par les lois canadiennes.

Comme les autorités d'application de la loi ont dû adapter leurs outils d'enquête en fonction des avancées technologiques, nos lois doivent faire de même.

Pourtant, comme nous l'ont indiqué plusieurs témoins, à l'heure actuelle, ni la Partie VI du *Code criminel* ni la *Loi sur la protection des renseignements personnels* ne sont

adaptées à l'ère numérique. La LPRPDE n'a également pas subi de mise à jour substantive depuis son adoption en 2000. Si les recommandations du Comité étaient adoptées, elles permettraient au gouvernement de faire cette mise à jour nécessaire.

Le Comité encourage donc le gouvernement du Canada à mettre en œuvre ses recommandations le plus rapidement possible, afin d'assurer un équilibre essentiel entre la protection du public, la protection de la vie privée et la confiance du public envers les institutions canadiennes.

ANNEXE A
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Commissariat à la protection de la vie privée du Canada	2022/08/08	30
Philippe Dufresne, commissaire à la protection de la vie privée du Canada		
Gregory Smolynec, sous-commissaire Secteur des politiques et de la promotion		
Ministère de la Sécurité publique et de la Protection civile	2022/08/08	31
L'hon. Marco Mendicino, C.P., député, ministre de la Sécurité publique		
Gendarmerie royale du Canada	2022/08/08	31
Dave Cobey, sergent conseiller gestion des dossiers techniques, Programme de gestion des dossiers techniques		
Mark Flynn, commissaire adjoint, police fédérale Sécurité nationale et police de protection		
Bryan Larkin, sous-commissaire Services de police spécialisés		
À titre personnel	2022/08/09	32
Daniel Therrien, avocat		
Conseil du Canada de l'accès et la vie privée	2022/08/09	32
Sharon Polsky, présidente		

Organismes et individus	Date	Réunion
À titre personnel	2022/08/09	33
Ronald J. Deibert, professeur en science politique, et directeur Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto		
Michel Juneau-Katsuya, expert et chercheur sur les questions de sécurité nationale et de renseignement		
Association canadienne des libertés civiles	2022/08/09	33
Brenda McPhail, directrice Programme de la vie privée, de technologie et de surveillance		
À titre personnel	2022/09/28	36
Michel Juneau-Katsuya, expert et chercheur sur les questions de sécurité nationale et de renseignement		

ANNEXE B
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Conseil du Canada de l'accès et la vie privée

The Citizen Lab

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions n^{os} 30, 31, 32, 33, 36, 43, 44 et 45) est déposé.

Respectueusement soumis,

Le président,
John Brassard